LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA
Av. Getúlio Vargas, nº 333, - Bairro Quitandinha,
CEP 25651-075, Petrópolis - RJ - http://www.lncc.br

Política de Segurança da Informação do LNCC-SANTOS DUMONT			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
03-PSISD	5.1	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022			**PUBLICADO EM**
5.1 - Liderança e comprometimento 5.2 - Política A.5.1 – Políticas de segurança da informação			21/10/2025

SUMÁRIO

1. OBJETIVO

1.1 Este documento é uma declaração formal do Laboratório Nacional de Computação Científica (LNCC) a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade e em sua guarda no que tange ao Supercomputador Santos Dumont.

1.2 Esta Política de Segurança da Informação foi elaborada pelo LNCC, com base: (i) nas normas técnicas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, (ii) na legislação vigente, (iii) na realidade e (iv) nos requisitos de negócio da entidade.

“A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos.”.

2. CAMPO DE APLICAÇÃO

2.1 Esta política se aplica a todas as unidades organizacionais do LNCC que atuam nos processos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001. Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e as partes interessadas.

2.2 Esta política aplica-se a todos os ativos no escopo do Sistema de Gestão de Segurança da Informação (SGSI) do Supercomputador Santos Dumont (SSD) e do CPD do Laboratório Nacional de Computação Científica (LNCC) que estão conectados ao SSD.

2.3 Esta política considera a abrangência da segurança da informação nos aspectos físico, lógico, comportamental, de pessoas, processos e tecnologias, preservando a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações do LNCC relacionados ao Supercomputador Santos Dumont ou sob sua salvaguarda, assim como a privacidade dos colaboradores.

2.4 A política aplica-se a todas as formas intelectuais e físicas de ativos de informação, sejam próprios, utilizados ou custodiados no LNCC e relacionadas ao Supercomputador Santos Dumont. Estas formas incluem hardware, redes, software e dados, sejam armazenadas e processadas em computadores, transmitida através de redes, impressos ou escritos em papel, enviada por fax, armazenados em meios legíveis por máquina (por exemplo, CD-ROM, fitas, tokens USB) ou falada em conversas e por telefone ou postada na Internet, por exemplo, em mídia social redes, chats ou wikis.

3. RESPONSABILIDADE

3.1 A responsabilidade pela elaboração, revisão e publicação desta norma é do Comitê de Segurança da Informação e Comunicação do LNCC.

3.2 A responsabilidade pela aprovação e cancelamento desta norma é do Diretor do LNCC.

3.3 Este documento é elaborado com o apoio do Gestor de Segurança da Informação.

4. DOCUMENTOS DE REFERÊNCIA

Os documentos a seguir, no todo ou em parte, são referenciados neste documento e fornecem requisitos, diretrizes ou orientações que são indispensáveis à sua aplicação. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do documento, incluindo emendas.

ISO/IEC 27000	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ABNT NBR ISO/IEC 27001	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

ABNT NBR ISO/IEC 27002	Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação
Política de Segurança da Informação do LNCC	Institui a Política de Segurança da Informação (PSI), no âmbito do Laboratório Nacional de Computação Científica (LNCC), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação

5. DOCUMENTOS COMPLEMENTARES

Os documentos a seguir serão utilizados, no todo ou em parte, para viabilizar a aplicação das informações documentadas do SGSI, devendo estar citados no corpo do texto normativo e disponíveis para uso.

Portaria GSI/PR nº 93, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)

6. SIGLAS

SGSI	Sistema de Gestão de Segurança da Informação
ISMS	Information Security Management System.
SSD	Supercomputador Santos Dumont.
TIC	Tecnologia da Informação e Comunicações

Nota: As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica (https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159).

7. TERMOS E DEFINIÇÕES

Colaboradores	No contexto deste documento, entende-se como colaborador quaisquer agente público, estagiário, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da instituição.

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Portaria GSI/PR nº 93/2021 e ISO/IEC 27000:2018, que devem ser interpretados somando-se as descrições. Em caso de divergência, prevalecem o termo e a definição estabelecidos na Portaria GSI/PR nº 93/2021.

8. PAPEIS E RESPONSABILIDADES

8.1 O Diretor do LNCC é o responsável pela aprovação e pelo cancelamento desta política.

8.2 O comitê de segurança da informação é o responsável pela análise crítica desta política.

8.3 Esta política se aplica a todos os colaboradores do LNCC, quais sejam: funcionários, servidores efetivos ou comissionados, estagiários, menores aprendizes, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações deste órgão no que tange ao

Supercomputador Santos Dumont.

8.4 A LNCC reconhece que uma gestão eficaz da segurança da informação é essencial para proteger seus ativos, manter a confiança das partes interessadas e assegurar a continuidade dos negócios. Por isso, todos os colaboradores devem estar comprometidos com a conformidade aos requisitos do Sistema de Gestão de Segurança da Informação (SGSI), adotando práticas que garantam a confidencialidade, integridade, disponibilidade e autenticidade das informações. A participação ativa de todos é fundamental para manter um ambiente seguro e alinhado aos objetivos estratégicos da organização.

8.5 Os colaboradores do LNCC envolvidos no escopo definido anteriormente devem ser informados acerca desta política de segurança.

8.6 No momento da divulgação desta política aos colaboradores, estes deverão ser informados de que, ao acessarem qualquer ativo incluído no escopo do SGSI, após tomarem ciência desta política, estarão reconhecendo que compreenderam seu conteúdo e concordam em cumpri-la integralmente.

8.7 Quando da identificação, os colaboradores e demais partes interessadas devem realizar a notificação de não conformidade, riscos e oportunidades de melhorias ao Gestor de Segurança da Informação (gsi@lncc.br).

9. ABNT NBR ISO/IEC 27001

9.1 Para assegurar os aspectos apresentados na seção 1

9.2 Objetivo, deve-se colocar em prática um processo de gestão de segurança da informação. Este processo, baseado na ABNT NBR ISO/IEC 27001 (“Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos”), é o chamado SGSI - Sistema de Gestão de Segurança da Informação (em inglês, ISMS - Information Security Management System).

9.3 O Sistema de Gestão de Segurança da Informação (SGSI) deve prever diversas ações, subprocessos, políticas e procedimentos de segurança, praticando a missão de reduzir continuamente os riscos à segurança das informações e aos ativos críticos de uma organização

10. CONTROLES E DIRETRIZES

10.1 Esta política define e padroniza o uso, o tratamento, o controle e a proteção das informações que possam causar impactos no desempenho financeiro, na participação no mercado e na imagem do LNCC, agregando valor à operação e eficiência na prestação de serviços ou no relacionamento com as partes interessadas, definidas no documento "Sistema de Gestão de Segurança da Informação (08-ISMS) ".

10.2 Esta política representa o comprometimento do Laboratório Nacional de Computação Científica em satisfazer os requisitos aplicáveis relacionados à segurança da informação, como a ABNT NBR ISO/IEC 27001 e a Política de Segurança da Informação do LNCC, bem como informações contratuais estatutárias e do processo.

10.3 A política inclui o compromisso com o processo da melhoria contínua do Sistema de Gestão da Segurança da Informação.

10.4 Os requisitos estatutários da “Política de Segurança da Informação do LNCC” são também parte obrigatória dessa política, de acordo com os requisitos do negócio do Supercomputador Santos Dumont e com as leis e regulamentações aplicáveis.

11. TREINAMENTO

11.1 Os colaboradores do LNCC devem receber orientações de Segurança da Informação. Para tanto, podem ser aplicadas ações de capacitação, conscientização e desenvolvimento, campanhas de comunicação via e-mail institucional ou via publicações nos murais de comunicação disponíveis nas dependências do LNCC.

11.2 Todos os colaboradores têm um papel fundamental na proteção das informações da organização. O LNCC deve orientar, capacitar e apoia continuamente os colaboradores para que atuem de forma consciente e responsável na identificação de riscos, no cumprimento das diretrizes de segurança e na comunicação de incidentes. Contribuir para a eficácia do Sistema de Gestão de Segurança da Informação (SGSI) é um dever coletivo, que fortalece a proteção dos dados e a resiliência institucional.

12. TRATAMENTO DE ISENÇÕES E EXCEÇÕES

12.1 Em conformidade com as normas ISO/IEC, todas as isenções e exceções aos controles de segurança da informação devem ser formalmente documentadas, justificadas e aprovadas por autoridade competente

12.2 O procedimento para tratamento de isenções e exceções deve seguir as seguintes diretrizes:

12.2.1 Solicitação Formal: Qualquer solicitação de isenção ou exceção deve ser submetida ao Gestor de Segurança Informação por escrito, contendo a descrição detalhada da necessidade, o controle de segurança afetado, o período solicitado e a justificativa baseada em análise de risco.

12.2.2 Análise de Risco: Toda solicitação será avaliada por meio de uma análise de risco documentada, considerando o impacto potencial na confidencialidade, integridade, disponibilidade das informações a privacidade do cidadão.

12.2.3 Aprovação: As isenções ou exceções só serão concedidas após aprovação formal pelo Gestor de Segurança da Informação. A decisão será baseada na análise de risco e na adequação das medidas compensatórias propostas.

12.2.4 Medidas Compensatórias: Quando aplicável, medidas compensatórias devem ser implementadas para mitigar os riscos associados à isenção ou exceção.

12.2.5 Registro e Monitoramento: Todas as isenções e exceções aprovadas serão registradas em um repositório centralizado, com detalhes sobre a justificativa, o período de validade e as medidas compensatórias. Essas aprovações serão revisadas periodicamente para garantir sua relevância e conformidade.

12.2.6 Prazo de Validade: Isenções e exceções terão um prazo definido, não superior a um ano, sujeito a revisões antes da renovação. Caso a necessidade persista, uma nova solicitação e análise de risco serão requeridas.

12.2.7 Comunicação e Conscientização: Os responsáveis pela solicitação serão informados sobre as condições de aprovação, responsabilidades e implicações. A equipe de segurança da informação promoverá a conscientização sobre este procedimento.

13. ANÁLISE CRÍTICA

Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, sempre que necessário, ao menos, uma vez ao ano.

14. HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	02/03/2020	Documento Inicial.
1.1	20/05/2020	Inclusão da classificação e tipo de acesso.
1.2	28/04/2021	Revisão da estrutura do documento e atualização do *template*.
1.3	18/05/2021	Revisão das seções 3.5 e 4.
2.0	01/06/2022	Análise crítica do documento; revisão do texto; ajuste nas nomenclaturas.
3.0	23/05/2023	Análise crítica do documento; atualização do template;
4.0	28/05/2024	Revisão e atualização das informações dos documentos e normativas citadas. Remoção da seção “Política de Transição”. Revisão do texto.
5.0	20/08/2025	Revisão e atualização das informações dos documentos e normativas citadas. Alinhamento com a versão de 2022 da norma ISO. Revisão do texto.
5.1	21/10/2025	Ajuste no formato do documento para o SEI

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação
Verificado por	Comitê de Privacidade e Segurança da Informação - Portaria LNCC/MCTI nº 420/2024	Membros do Comitê de Privacidade e Segurança da Informação
Aprovado por	Wagner Vieira Léo	Diretor Substituto do LNCC

Documento assinado eletronicamente por **Luis Rodrigo De Oliveira Gonçalves**, **Gestor de Segurança da Informação**, em 21/10/2025, às 15:39 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Wagner Vieira Léo**, **Diretor do Laboratório Nacional de Computação Cientifica substituto**, em 22/10/2025, às 09:09 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Bruno Alves Fagundes**, **Chefe do Serviço de Suporte de Sistemas e Redes**, em 22/10/2025, às 15:43 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.